Application No.: 10/656,570 Docket No.: 17245/007004

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) An intrusion secure personal computer system comprising:

a ~~CPU~~central processing unit;

a data storage means;

a memory means;

a[[n]] primary operating system;

a virtual machine operating system providing an isolated secondary operating environment functioning separate from the primary operating system and controlling operations of the personal computer system within the isolated secondary operating environment; and

at least one input/output (I/O) connection in operative communication with an external data source,

wherein the personal computer system is secured from malicious code contained in a file downloaded from the external data source.

2. (Currently Amended) The computer system of claim 1, wherein the external data source is a global computer network.

3. (Canceled)

4. (Currently Amended) The computer system of claim [[3]] 1, wherein the external data source ~~other than a global computer network~~ is at least one external data source selected from the group consisting of: a computer workstation, a personal-type computer, a computer dock, a local area network, an intranet, and a wide area network.

5. (Currently Amended) The ~~intrusion secure~~ computer system of claim 1, wherein the virtual machine operating system comprises software for defining a virtual machine environment in memory and a virtual drive in storage, and operational control software limiting operative communication with the external data source to the virtual machine environment and the virtual machine drive.

6. (Currently Amended) A method for securing a personal computer system from intrusion from an external data source comprising the steps of:

providing an intrusion secure personal computer system of claim 1;

initiating an external data source interface session, ~~and~~ wherein initiating the external data source interface session causinges activation of a virtual machine operating system of claim 1 and defininges a virtual machine environment in memory and a virtual drive in storage; and

establishing connectivity with the external data source under control of the virtual machine operating system to isolate operative communication with the external data source to the virtual machine environment and the virtual drive to secure the computer system from intrusion from the external data source.

7. (Currently Amended) A software application stored as executable instructions on a computer readable medium and installable on a personal computer, ~~the software protecting the computer's primary data files from being accessed by malicious code from an external data source, the software~~ comprising:

executable instructions ~~computer code~~ for an isolated operating environment; and

executable instructions ~~computer code~~ for a secondary operating system functional within the isolated operating environment on the personal computer,

wherein primary data files of the personal computer are prevented from being accessed by malicious code from an external data source.

8. (Currently Amended) The software application of claim 7, wherein the isolated operating environment executable instructions ~~computer code~~ include[[s]] primary operating system (POS) permission code for modifying the POS permissions.

9. (Currently Amended) The software application of claim 8, wherein the secondary operating system executable instructions ~~computer code~~ include[[s]] primary operating system (POS) permission code for modifying POS external data source related access permissions.

10. (Currently Amended) The software application of claim 9, ~~wherein the secondary operating system computer code includes POS permission code for modifying POS external data source related access permissions,~~ wherein the external data source is at least one source

selected from the group consisting of a network node, an external data device, and an I/O device.

11. (Currently Amended) The software application of claim 8, wherein the secondary operating system executable instructions ~~computer code~~ include[[s]] primary operating system (POS) permission code for modifying POS internet related permissions.

12. (Currently Amended) The software application of claim 8, wherein the secondary operating system executable instructions ~~computer code~~ include[[s]] primary operating system (POS) permission code for modifying POS Hnet permissions.

13. (Currently Amended) The software application of claim 7, wherein the isolated operating environment executable instructions ~~computer code~~ include[[s]] installation code for checking and setting the isolated operating environment.

14. (Currently Amended) The software application of claim 13, wherein the isolated operating environment executable instructions ~~computer code~~ include[[s]] installation code for checking and setting the isolated operating environment, wherein the installation code checks for ~~the~~ a current installation condition of the software application.

15. (Currently Amended) The software application of claim 14, ~~wherein the isolated operating environment computer code includes installation code for checking and setting the isolated operating environment,~~ wherein the installation code copies any files from the software application as are necessary in view of ~~the~~ checking for the current installation condition of the software application.

16. (Currently Amended) The software application of claim 14, ~~wherein the isolated operating environment computer code includes installation code for checking and setting the isolated operating environment,~~ wherein the installation code establishes short-cuts as are necessary in view of ~~the~~ checking for the current installation condition of the software application.

17. (Currently Amended) The software application of claim 7, wherein the isolated operating environment executable instructions ~~computer code~~ include[[s]] code checking and setting the isolated operating environment start up requirements.

18. (Currently Amended) The software application of claim 17, wherein ~~the isolated operating environment computer code includes code checking and setting~~ the isolated operating environment start up requirements ~~regarding~~ include "freshness" of ~~the~~ secondary operating environment (SOE) files, allocation of volatile memory to the SOE, allocation of data storage to the SOE, READ ONLY condition of the primary operating system partitions and connections, state of intranet activity, READ ONLY condition of user access to primary operating system partitions.

19. (Currently Amended) The software application of claim 7, wherein the isolated operating environment executable instructions ~~computer code~~ include[[s]] code checking and setting the isolated operating environment runtime requirements.

20. (Currently Amended) The software application of claim 19, wherein ~~the isolated operating environment computer code includes code checking and setting~~ the isolated operating environment runtime requirements are set to provide at least two run modes.

21. (Currently Amended) The software application of claim 19, wherein ~~the isolated operating environment computer code includes code checking and setting~~ the isolated operating environment runtime requirements are set to provide at least a run mode with inet access and a run mode without inet access.

22. (Currently Amended) The software application of claim 7, wherein the isolated operating environment executable instructions ~~computer code~~ include[[s]] code checking and setting the isolated operating environment exit requirements.

23. (Currently Amended) The software application of claim ~~22~~ 7, wherein the isolated operating environment executable instructions ~~computer code~~ include[[s]] code checking and setting the isolated operating environment exit requirements ~~includes~~ comprising disconnecting [[(the]] a secondary operating environment (SOE) from ~~the~~ an inet, closing ~~the~~ a node interface, freeing ~~the~~ an SOE volatile memory allocation, flushing ~~a the~~ temporary data storage allocation, disconnecting from any SOE files and partitions, refreshing SOE boot file, and restoreing an intranet connection.

24. (Currently Amended) The software application of claim 7, wherein the isolated operating environment executable instructions ~~computer code~~ include[[s]] code checking and setting the isolated operating environment requirements.

25. (Currently Amended) The software application of claim 7, wherein the isolated operating environment executable instructions ~~computer code~~ include[[s]] code checking and setting the isolated operating environment requirements, including: allocating and connecting to a region of volatile memory for ~~the~~ a secondary operating environment (SOE), allocating and connecting to a data storage space, providing a connection to a ~~CPU~~central processing unit of the personal computer, connecting to an external data source node, providing a connection to a video card of the computer, providing a connection to a sound card of the computer, providing a connection to a printer of the computer, providing a connection to a mouse and a keyboard of the computer, and forming a network bridge between the secondary operating system of the SOE and the primary operating system of the personal computer.

26. (Currently Amended) A security method for protecting a personal computer from malicious code derived from an external data source comprising the steps of:

loading a software application installable on the personal computer, wherein the software application ~~for~~ protect~~sing~~ the personal computer's primary data files from being accessed by malicious code from ~~an~~ the external data source;

installing the software application on the personal computer, the installed application defining an isolated operating environment including a secondary operating system, the secondary operating system functioning in conjunction with and separate from a primary operating system on the personal computer, and the installed application defining primary operating system permission codes to limit access to a node connectable to ~~an~~ the external data source to the isolated operating environment under control of the secondary operating system;

initiating an external data source interface session via the node within the isolated operating environment, and allocating a volatile memory space and a temporary data storage space to the secondary operating system for the duration of the session; and

establishing connectivity with the external data source via the node under control of the secondary operating system to isolate operative communication with the external data source to the isolated operating environment, and protecting the personal computer from malicious code derived from the external data source.